National Park Service
Point of Sale System (POSS)

Privacy Impact Assessment

21 June 2013

NPS Point of Sale System (POSS)
Privacy Impact Assessment

National Park Service
Recreation Fee Program
1201 I Street, N.W.
Washington, D.C. 20005

SECTION I

Privacy Impact Assessment for the Point of Sale System (POSS)

Name of Project: Point of Sale System (POSS)
Bureau: National Park Service
Project's Unique ID: DOI_NPS_216

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

Who is the Bureau/Office Privacy Act Officer who reviewed this document? (Name, organization, and contact information).

Felix A. Uribe
NPS Privacy Officer
Bureau Chief of Information Security Office
1201 Eye St. NW, Washington, DC 20005
Telephone: 202-354-6925
Email: felix_uribe@nps.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes, the system will contain limited information on members of the public to be used in completing credit card transactions used by members of the public in paying recreation fees. This functionality is required for any business activity that accepts credit cards for payment (such as the National Park Service) and is implemented in accordance with the Payment Card Industry (PCI) Data Security Standards, which is the organization that governs credit card payment applications.

The amount of information retained is the absolute minimum required to securely process and account for visitor credit card payments, and allow for chargeback functionality when appropriate. The only data element that is retained that is identifiable to an individual is the "cardholder name" field – the name that appears on an individual's credit card. No address or telephone number is captured or retained. Retaining of this information is essential in order to preserve the National Park Service's right to respond to a chargeback request.

In addition, access to credit card information, before nightly purging (and on the HQ server) will be strictly controlled. Access to all sensitive functions of the POSS, including the credit card transactional records, is tracked and will be routinely audited. Since parks currently process credit cards for visitor fees, this capability and responsibility is not new; it simply replaces existing technology.

The actual credit card number (PAN) will never be used, stored, displayed, or transmitted in plaintext (unencrypted) form, under any circumstances in the system.

a. Is this information identifiable to the individual11?

(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Only the cardholder name field, for the limited purpose described above.

b. Is the information about individual members of the public?

(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

Yes, but only during and for the purpose described above. For members of the public (park visitors) who choose to pay by credit card, the details of that transaction (including credit card number and cardholder name) will be gathered at the point of sale. This is required for any point of sale system in which people are allowed to pay by credit card.

Security controls associated with this information are described in section B.1, above.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes, but only in that all financial transactions created in the course of business must be traceable to an individual employee who generated the transaction.

2)What is the purpose of the system/application?

1 1 "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

The National Park Service collected over $160M in FY2006 in Recreation Fee Revenues at 270 sites throughout the United States. Of the 270 park units, approximately 216 collected fees through a combination of entrance, special use, transportation, or reservation fees and 54 sites collected fees solely through annual pass sales.

The NPS does not have a servicewide or standardized point of sale (POS) system at all 270 sites. Each park unit maintains independent procurements for the configuration, installation, maintenance, and troubleshooting of equipment and software. The remaining 214 units use cash registers, canisters (payment through honor system metal drop boxes) or manual processes with no automated record keeping, data collection or reporting capability.

At the time of this update of the PIA, POSS has been deployed at four parks.

The significant volume of servicewide fee revenue, combined with technology trends and expectations from the public and laws such as the Clinger-Cohen Act, which provides guidance for IT projects, establishes the need for a Service-wide Point-of-Sale System for the National Recreation Fee Program revenues. This project is intended to allow the NPS to collect and manage revenue transactions and visitor demographics down to the transaction level, as well as provide for increased training efficiency across the service through standardized equipment and hardware options. Therefore, the mission of this project is to procure a standardized, yet flexible, Servicewide fee collection Point-of-Sale System (POSS), enabling effective and efficient collection, accounting, and centralized reporting of NPS fee revenues. The system will simplify and standardize the procurement, training, installation and support of the equipment and software.

POSS provides the **Park Fee Programs** with:

- Centralized support for all aspects of the installation and operations of the servicewide POSS.

- POS units that shall:
  - Conduct transactions rapidly and efficiently with visitors to the park.
  - Accept and process cash, check, credit-card, and vouchers payments.
  - Accept and record serialized inventory controlled items (i.e. passes).
  - Deposit fee revenue efficiently into the Treasury designated programs and provide transaction data nightly for the timely upload to the Service's financial systems.
  - Capture transaction details and statistical metrics.
  - Report revenues and statistical metrics effortlessly and accurately fee into a Service-wide database for analysis.
  - Support multiple types of fee collection (e.g. entrance, campground, and tour).
  - Support fee collection activities with varying levels of infrastructure capabilities (network access, data transfer capabilities, reliable electrical power).
  - Maintain inventory of serialized products for sale (by system-wide unique inventory location identifier)

- An architecture that is extensible to future needs, compliant with all Federal Government and NPS security standards, based on Commercial Off-The-Shelf (COTS) technology, allows the NPS maximum flexibility in hardware and peripheral choice, and provides the NPS the maximum value with respect to benefits and total cost of ownership.

Upon implementation of this project, the **National Recreation Fee Program**, **Regional Fee Mangers**, **Park Superintendents and Fee Program Managers** will have:

- Servicewide standards for detailed fee revenue collection and reporting.

- Immediate and ready access to a current and complete data warehouse of fee revenue and demographic data for analysis and reporting.
- Ability to accurately and efficiently generate recurring and ad hoc financial reports.

Upon implementation of this project, **visitors** to the parks will have the ability to pay for park-specific recreation fees through:

- A consistent, smooth, fast and efficient transaction at the fee collection station, regardless of method of payment.
- The payment of cash, check, credit card, house charge, pre-purchased items, or vouchers.

The successful implementation of the servicewide POSS will result in:

- Improved management of fee revenue.
- Accurate accounting for fee revenues.
- Streamlined procurement and IT coordination for the installation of POS units.
- Improved accountability and reduced potential for fraud.
- Improved consistency and availability of servicewide metrics and fee collection data.

3) What legal authority authorizes the purchase or development of this system/application?

The Federal Lands Recreation Enhancement Act (REA)-- From the 2005 Consolidated Appropriations Act (PL 108-447) signed into law by President Bush on December 8, 2004 establishes that the Secretary has the authority to establish, modify, charge, and collect recreation fees at federal recreational lands and waters as provided in section 16 USC 6802 section 803. This law supersedes the Recreational Fee Demonstration Program (Fee Demo) in 1996 and the Land and Water Conservation Act of 1965 (LWCA) (16 USC § 4601-4; PL 88-578).

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Individuals who attempt to pay by credit card for recreational fees at a park (including fees for entrance to a park, purchase of a park or interagency pas, fees, backcountry permits, or tours).

Individuals who use their annual pass to re-enter the park and the serial number of the pass is captured.

Direct employee activities in the system are also captured, and will be identifiable by the employee's name or other user identifier.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Direct swipe of the magnetic stripe of a credit card into a Point of Sale unit when a visitor tenders a credit card for payment of recreation fees; or manual entry of the information from a credit card, if the Point of Sale hardware is unable to read the information off of the magnetic stripe of the credit card.

Direct swipe of an annual pass or re-entry will capture the serial number.

b. What Federal agencies are providing data for use in the system?

None

c. What Tribal, State and local agencies are providing data for use in the system?

None

d. From what other third party sources will data be collected?

Future Integration – Financial Data from Automated Fee Machines, Datasym Cash Registers, NRRS Field Manager Sales and inventory quantities. There will be no PII transferred.

e. What information will be collected from the employee and the public?

- For members of the public, only that information that is necessary to accept, process, settle, and document a transaction via credit card, and is permissible under Payment Card Industry (PCI) Data Security Standards, version 2.0:

  1) Account number, also known as PAN (Primary Account Number). This is encrypted in all files, including the database, using AES256 encryption, as per PCI requirements. This information is not available in plaintext (unencrypted) form to **any** user of the system.

  2) The Expiration date.

  3) Account holders name, which we can print on the receipt if so configured.

- As per PCI DSS guidelines, the system does NOT store in any form track data, CVV, CVV2 or CID numbers.

The personally-identifiable credit card information stored is the absolute minimum required to process credit card transactions and respond to chargeback requests. For more information on chargeback requests and their processing, see the Visa Rules for Merchants (http://usa.visa.com/download/merchants/rules_for_visa_merchants.pdf). All PII data is automatically purged from point of sale units and park servers. Additional security controls

associated with this data are described in section B.1, above.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOI records be verified for accuracy?

The credit card transaction will be authorized, either immediately (if connectivity permits) or in batches through the Treasury's Card Acquiring Services, which is used for authorization of all credit card transactions for payments to the Federal Government. Credit cards will be captured at the point of sale, but will be settled once per day.

b. How will data be checked for completeness?

Through the authorization process, as stated above.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Through the authorization process, as stated above. After the transaction is settled, the only use for the data is to respond to chargeback requests.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The captured fields consist of:

1) Account number, also known as PAN (Primary Account Number). This is encrypted in all files, including the database, as per PCI requirements. This information is not available in plaintext (unencrypted) form to **any** user of the system.
2) A truncated version of the account number. We store every other digit of the account number so that we can do searches

by account number. This is permitted under PCI rules.
3) The Expiration date.
4) Account holders name, which we can print on the receipt if so configured.

The system does NOT store track data, CVV, CVV2 or CID numbers.

The requirements associated with each of these data fields can be found in the PCI Data Security Standards (version 2.0) at: https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v2.pdf.

The payment application used by POSS, In The Black Retail Suite version 1.20, was validated as compliant with PCI Data Security Standards on 7/12/2013 (reference number 09-11.00340.001). Refer to:

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php?agree=true

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes; otherwise, visitors would be unable to pay recreational fees via credit card. Such information is currently being captured; just not handled and processed in a systematic form.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No

3) Will the new data be placed in the individual's record?

No

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

Not about the public.

The system may be used to generate reports on employees (fee collectors) in terms of their sales activities, including cash drawer shortages and overages.

5) **How will the new data be verified for relevance and accuracy?**

The employee sales activities are validated during the operational procedures of validating shifts during a remittance and deposit.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Appropriate and authorized User Roles will be assigned for access employee activities. Access control model is documented in the POSS System Security Plan (SSP).

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

User roles and permissions are fundamental to the design and implementation of the POSS. Only properly authenticated and authorized users shall have permissions to generate access any data in the system. See the System Security Plan for details. The system will receive Authorization to Operate before being deployed in the field (and received Authorization to Operate 2012-03-23).

8) **How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

In the case of a chargeback, the individual's credit card transactions can be retrieved by the authorization number of the original transaction or the visitor's credit card number, in order to respond to the chargeback request. PCI Data Security Standards permit the storage of every other digit (alternating digits) of the PAN, in order to allow a search on the card number, if a visitor submits a chargeback request.

Data is not retrievable by an individual identifier.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Pass users may be tracked by pass use, but no information is collected or stored that would allow this to be traced to an individual.

Employees' sales totals (including cash drawer overages and shortages) may be retrieved and reported on.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

- Visitors who are required to provide their credit card may pay by a different method (cash, personal check, travelers check).

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

- The system will be implemented in a consistent and standardized manner across the NPS, and uniform standard operating procedures will be created. Visitor Use Assistants (Fee Collectors) and others using the system will be trained before use, and are subject to continuous monitoring and auditing, for accountability and security reasons.

2) What are the retention periods of data in this system?

- Credit card information will be stored to the degree and in the manner described in order to respond to chargeback requests. Visa regulations strongly recommend that documentation be retained for one year. For that reason, the required credit card data will be stored in the system for one year.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

- All data within the system will be stored indefinitely. After the retention period it will be archived and stored on backup tapes per the backup procedures at NISC.

- The procedures will be documented in the standard operating procedures for the system, which will be available to and required reading for any employee using the system.

4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

- No

5) How does the use of this technology affect public/employee privacy?

- For visitors there is no change. Visitors have always and will always have to present their credit card for authorization and processing if they choose to pay by credit card. Visitors may always pay with cash if they wish not to have their credit card data recorded and processed.

- Employees who work in fee collection already are subject to a significant amount of monitoring, both for fraud prevention and detection, and for their own personal security. Monitoring includes use of cameras and microphones, random or planned audits, and use of two employees at a time to process or collect cash. This system will not change the amount of monitoring that employees already undergo.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

- Not for members of the public.

- The system can be used to monitor employees only in the sense that all employee actions on the Point of Sale system will be logged, and are subject to audit at any time, either by park fee staff, or by law enforcement.

7) What kinds of information are collected as a function of the monitoring of individuals?

- Only actions in the system itself, as used by individuals in using the system as part of their job. There is no reasonable expectation of privacy on the park of employees using the Point of Sale system for their jobs.

8) What controls will be used to prevent unauthorized monitoring?

- Reports and data requests from the system are themselves logged and subject to audit.

Separation of duties and audit will provide adequate controls to prevent unauthorized monitoring. Employees are already required per NPS policy to sign and accept the rules of behavior for NPS IT systems along with Federal Information Systems security training, and Privacy Act training. In addition, Fee Collectors are required to sign the Designation and Revocation of Fee Collection form.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

None is required, as the system does not permit individual records from the public to be retrieved by an individual identifier.

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

N/A

F. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)

- Contractors responsible for the development, maintenance and/or administration of the system.
- NPS IT staff, who may also be responsible for installing or administering POS units
- Visitor Use Assistants (Fee Collectors), Fee Supervisors and Managers, and others directly responsible for the collection, deposit, reconciliation, and reporting on fee revenues
- WASO and Regional Recreation Fee Program office staff who may use the system for reporting

- Accounting Operations Center staff who may use the system for reporting.

All employees and contractors who have access to the system will have a full background investigation, and will already have network access to the DOI network.

Note that the credit card number (PAN) will never be available to **anyone** in plaintext (unencrypted) format for any reason.

PII will only be available to specifically authorized personnel who have a need to know, and have been granted the appropriate clearance level.

2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

- Standard operating procedures will be followed strictly, when granting access to the system. Users will only be given access to that part of the system required to perform their jobs.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

- User access to the system will be restricted to that required to perform their job (on a need-to-know basis). Field staff will not have access to any data other than that from their own park. Ability to change data in the system (insert, update, delete) will be strictly controlled, and all such actions logged and subject to multiple levels of audit.
- Note that the credit card number (PAN) will never be available to **anyone** in plaintext (unencrypted) format for any reason.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

- Credit card information will only be retained in the HQ database after settlement.
- The POSS has a robust, role-based security model.
- Access to all sensitive functions of the POSS, including the credit card transactional records, is tracked and will be routinely audited. All employees with access will have received IT security and Privacy Act training in advance of being given access.
- Since parks currently process credit cards for visitor fees, this capability and responsibility is not new; it simply replaces existing technology.
- The actual credit card number (PAN) will never be used, stored, displayed, or transmitted in plaintext (unencrypted) form, under any circumstances.
- All usage of the system will be strictly monitored as per the System Security Plan. All activities on the system are logged and audited.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

- Yes and yes. The system developer is under contract for maintenance of the system. Personnel with access to NPS systems or data have received background clearance and network credentials from the NPS. Privacy Act contract clauses have been inserted into the contract.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

- Credit card transactions are authorized and processed using the Treasury Card Acquiring Services. The POS units will transmit the required data in encrypted form as per standard Federal Government procedures. An Interconnection

Security Agreement / Memorandum of Understanding (ISA/MOU) is in place for this interface.

- Other system interfaces to the system do not involve information on individuals at all.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

- The NPS POSS Security Manager and the contractor providing support for the system will be responsible for the secure transmission of credit card data, as per standard industry security controls, to the Card Acquiring Services, processing network.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

- US Department of Treasury, through Card Acquiring Services, only for the purpose of authorizing and processing credit card payments from visitors.

9) How will the data be used by the other agency?

- Only in processing the credit card transaction.

10) Who is responsible for assuring proper use of the data?

- The NPS POSS Security Manager for POSS is responsible for ensuring that the credit card information is securely captured from the visitor, securely transmitted through for processing, and deleted from the POS.